UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
FORT WAYNE DIVISION

JUMPSTART COMMUNICATIONS LLC, Plaintiff, vs. RYAN V. JUMPER and THE JUMPER GROUP LLC F/K/A JUMPSTART COMMUNICATION LLC, Defendants.	)	Magistrate Judge Susan L. Collins Case No. 1:24-cv-00447

STIPULATED PROTECTIVE ORDER GOVERNING IMAGING AND INSPECTION OF DEFENDANTS' ELECTRONIC DEVICES, PROTECTION OF CONFIDENTIAL AND PRIVILEGED INFORMATION, AND PRESERVATION OF PRIVILEGE IN THE EVENT OF PRODUCTION OF PRIVILEGED MATERIAL

IT IS STIPULATED AND AGREED by counsel for Plaintiff and Defendants, and hereby ORDERED that, pursuant to Rule 26 of the Federal Rules of Civil Procedure, the following procedure shall govern the inspection of Defendants' electronic devices during these proceedings.

I. PRESERVING CONTENT AND ARTIFACTS ON RELEVANT ELECTRONIC DEVICES

A. Defendants will make any agreed-upon and/or court ordered computers, cell phones, cloud repositories and other sources of electronic data (hereinafter the "Relevant Electronic Devices") that Defendants own, control, and/or possess available at a mutually convenient date and time to allow Plaintiff's expert, or the expert's representative, to make a forensic copy of the hard drives, memory, and/or storage media installed in each of the Relevant Electronic Devices.

B. There is resident on each of the Relevant Electronic Devices data that is relevant to the claims or defenses of any party. All relevant data can be categorized as content and/or artifact data. Content data includes all data generated by a human, while artifact data is generated by a computer.

C. Preservation of the content and artifact data resident on the Relevant Electronic Devices does NOT include any searching. Preservation will be completed by

ArcherHall creating on its evidentiary electronic media a forensic copy (hereinafter "Forensic Image") of the hard drives, memory, and/or storage media installed in each of the Relevant Electronic Devices. Once created, the Forensic Images permit the extraction and analysis of content and artifacts in the manner described in Section II below, without causing any changes to the content or artifacts.

D. As ArcherHall creates each Forensic Image, ArcherHall will verify that each Forensic Image is an exact, reliable copy of the hard drives, memory, and/or available storage media installed in each of the Relevant Electronic Devices. ArcherHall's verification may include calculating a "digital fingerprint" (MD5/SHA1 or other industry standard algorithm hash).

E. Defendants' counsel, or his authorized representative, may observe the creation of each Forensic Image of the hard drives, memory, and/or storage media installed in each of the Relevant Electronic Devices.

F. ArcherHall, and its representatives, will perform all work using usual and customary practices and industry standards and will create each Forensic Image using a forensically sound and defensible protocols.

II. EXTRACTING RELEVANT CONTENT, AND IDENTIFYING AND ANALYZING RELEVANT ARTIFACTS

A. ArcherHall will create a Digital Forensic Analysis Team whose members will be responsible for the identification and extraction of relevant content from the Forensic Image(s) and for the identification and interpretation of relevant artifacts. The names and curriculum vitae of each member of the Team will be made available upon request.

B. No ArcherHall personnel will "browse" the Forensic Image(s), hoping to find relevant content and/or artifacts. One or more members of The Digital Forensic Analysis Team will analyze the volume, type, format, file characteristics, and properties of data resident upon the Forensic Images and perform the following analytic functions:

i. explain to the parties any technological characteristics of the data that ought to be considered by the parties so that parties will be able to read, review, redact, produce, and authenticate relevant content;

ii. Recommend, where applicable, processing of some data by third parties;

iii. Recommend defensible search protocols, including predictive coding techniques, to properly reduce the amount of manual review necessary and avoid waiver of privilege;

iv. Apply its expertise to identify in all areas of each Forensic Image, including in-use space (allocated areas), slack space and unused space (unallocated areas), relevant content and/or relevant artifacts;

C. The analysis of the Forensic Images will take place at ArcherHall. Since the Forensic Images can be made in the presence of Defendants' counsel, and subsequently verified via the MD5 (or other appropriate) hash checksum, the presence of Defendants' counsel during the analysis of the Forensic Images is unnecessary. Since much of the analysis and searching of Forensic Image(s) can be carried out in an automated, unattended fashion, if Defendants' counsel insists on observing the analysis, he/she agrees to pay ArcherHall's fees for the time spent attending to the analysis of the Forensic Image.

D. ArcherHall frequently agrees to protocols and procedures to protect privileged content and to assist in the production of relevant Content and Artifacts. ArcherHall will use its digital forensic expertise to assist in the creation of technically feasible protocols or procedures to safeguard against the waiver of privilege due to inadvertent production of documents subject to claims of attorney-client and/or work product privilege.

E. ArcherHall shall report the results of its analysis in the following manner:

i. From time to time**,** ArcherHall shall prepare the following types of reports: a Report of Relevant Content, an Abstract of Select Provisions of the Report of Relevant Content (hereinafter the "Abstract"), and a Report of Relevant Artifacts.

ii. Relevant Content. The Report of Relevant Content will include in native format (or in the format(s) as agreed upon by the parties after consulting with ArcherHall) electronic copies of all files identified by the search and analysis conducted in paragraph IIBiv, supra. Where proper, relevant content in native file format can be converted to a file format such as pdf or tiff, which files shall be linked to the metadata related to the native file. ArcherHall will explain technologically feasible methods by which relevant content and metadata can be provided to Defendants for review, including any issues related to the electronic file review capabilities of Defendants.

iii. Abstract. The Abstract shall be limited to a statement of the number of pages in the Report of Relevant Content, the procedures and processes used by ArcherHall to complete its analysis of relevant content and artifacts, the number of pieces of relevant content data included in the Report of Relevant Content, and authentication information related to the Relevant Electronic Devices.

iv. Artifacts. The Report of Relevant Artifacts shall include ArcherHall's

opinion and all artifacts related to the manner in which Relevant Electronic Devices were used, the state of the data resident upon the Relevant Electronic Devices (including certification of completeness of data and integrity of data), and any other relevant computer usage issue.

v. ArcherHall shall submit the Abstract and Report of Relevant Artifacts by providing a copy to all parties. ArcherHall shall submit the Report of Relevant Content by providing a copy to Defendants' counsel only.

vi. Within fifteen business days of receiving an electronic copy of the Report of Relevant Content, Defendants' counsel will redact the report, prepare a log identifying the items in the Report of Relevant Content that counsel has redacted and the grounds therefore (privilege, relevance, etc), and provide a copy of the Redacted Report of Relevant Content on counsel for Plaintiff. The Redacted Report of Relevant Content will be served on counsel for Plaintiff in the same electronic format as it was created by ArcherHall, except redacted electronic copies of relevant content will be produced in pdf or some other acceptable format linked to the metadata contained in the native, unredacted, file. The purpose of this provision is to cause all non-redacted, relevant data to be produced in native format with metadata attached to the electronic files, and all redacted relevant data to be produced in pdf, tiff, or some other format that protects the redaction from being recovered.

vii. In some cases, circumstances may require that relevant content and artifacts are reported seriatim. In this event, an index of items included in each "rolling" production of relevant content and relevant artifacts (hereinafter the "Rolling Index of Content and Artifacts") shall be created and maintained by ArcherHall. The Rolling Index of Content and Artifacts shall append the items included in each rolling production, so that the index continues to expand with each "rolling" production.

viii. Each rolling production of relevant content shall be provided to Defendants' counsel only, who shall redact the content for privilege and prepare a log as set forth in paragraph vi above.

ix. Each rolling production of relevant artifacts shall be provided to Plaintiff's counsel and Defendants' counsel simultaneously by ArcherHall.

III. CONFIDENTIAL INFORMATION

A. Any information contained on Forensic Images that is not reported by ArcherHall shall be considered confidential information and subject to the provisions of the parties' Stipulated Protective Order. Any data reported by ArcherHall that is claimed by Defendants to be subject to attorney-client privilege shall be treated as

confidential information. ArcherHall and its representatives agree not to reveal to, or discuss with Plaintiff any confidential information absent a modification of this Order or other court Order. ArcherHall agrees to subject itself to the jurisdiction of the Court, and the parties agree that ArcherHall has standing to request Court intervention to protect ArcherHall's economic, reputation, and/or legal interests in this matter.

B. The inadvertent or intentional disclosure by ArcherHall or any representative of ArcherHall of confidential information shall not be deemed a waiver in whole or in part of Defendants' claim of confidentiality or protection under this Order, either as to specific information disclosed or as to any other information relating thereto or on the same or related subject matter. Counsel for the parties shall, in any event, upon discovery of inadvertent error, cooperate to restore the confidentiality and protection of the confidential information.

C. Nothing in this Order shall prevent the parties from using relevant, non-confidential information derived from the inspection of Defendants' electronic devices in connection with the trial, hearings, depositions, motions, memoranda or other proceedings in this action. Nor shall this Order prevent the parties from obtaining from ArcherHall by way of testimony or affidavit, explanations of the process, procedure, or results used or obtained by ArcherHall.

IV. PRIVILEGE REVIEW AND PRODUCTION

A. The Court is aware that the Defendants must conduct a privilege review of the relevant data prior to producing same to Plaintiff's counsel. In the event that Defendants conclude that, due to the volume of relevant data, it cannot complete the privilege review of all relevant data within fifteen business days, Defendants may request a hearing at which the Court will review the steps taken by the Defendants to review the relevant data, the volume of data subject to review, and the resources of Defendants. Based upon the Court's independent review of the scope of discovery permitted, the reasonableness of the procedures used by Defendants to identify privileged matter, and the amount of time that the Court will allow Defendants to complete the review, the Court may compel the production of all relevant data with less than full privilege review and find that such a production does not waive the claim of privilege for any material in accordance with the procedure and case law enunciated in *Hopson v. The City of Baltimore* 2005 WL 3157949 (D.Md), and the "compelled disclosure" theory enunciated in *Transamerica Computer Co*. v. IBM, 573 F.2d 646 (9th Cir. 1978)

IT IS SO ORDERED.

DATE: _____

_____
UNITED STATES MAGISTRATE JUDGE

Approved and Agreed to By:

/s/ Carrie E. Sheridan
Carrie E. Sheridan #38703-02
J. Blake Hike #28601-02
Brendan C. Ruff #39003-41
CARSON LLP
301 W. Jefferson Boulevard, Suite 200
Fort Wayne, Indiana 46802
Telephone: (260) 425-9777
Email: sheridan@carsonllp.com
hike@carsonllp.com
ruff@carsonllp.com

Attorneys for Plaintiff

/s/ David E. Bailey (per 1/31/2025 email authority)
David E. Bailey #21527-02
Audrey M. Van Gilder #35664-49
FLETCHER VAN GILDER, LLP
436 E. Wayne Street
Fort Wayne, Indiana 46802
Telephone: (260) 425-9777
Email: bailey@fvglaw.com
amvangilder@fvglaw.com

Attorneys for Defendants

Exhibit 1